TITLE:

一般化量子チューリング機械と部分再帰関数に関する問題について (非可換解析とミクロ・マクロ双対性)

AUTHOR(S):

入山, 聖史; 大矢, 雅則

CITATION:

入山, 聖史 ...[et al]. 一般化量子チューリング機械と部分再帰関数に関する問題について (非可換解析とミクロ・マクロ双対性). 数理解析研究所講究録 2008, 1609: 102-109

ISSUE DATE:

2008-07

URL:

http://hdl.handle.net/2433/140011

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録
第1609巻 2008年 102-109

一般化量子チューリング機械と部分再帰関数に関する問題について

入山聖史，大矢雅則
東京理科大学理工学部情報科学科

概 要

Ohya，Masuda，VolovichによりSAT問題に対する量子アルゴリズムが提案され（OMV-SATアルゴリズム），さらにOhya, Iriyamaによる一般化量子チューリング機械（GQTM）による記述がなされたことにより，言語クラスNPは多項式時間で解けるクラス（BGQPP)に属することが分かった．しかしながら，全ての古典アルゴリズムに対して，効果的な量子アルゴリズムが存在するかということは明らかではない．

本講演では，量子アルゴリズムの数理モデルである一般化量子チューリング機械の定義を説明し，部分再帰関数の計算を量子アルゴリズムを用いて効果的に実行しようとするときの，計算の複雑さについて議論を行う．

1 序

我々はヒルベルト空間上の量子チャネルと密度作用素を用いて，一般化量子チューリング機械（GQTM）を定義した[7, 9]．これは，量子アルゴリズムとして，観測過程やその他の物理過程を含む形での一般化であり，これにより，量子力学を原理とした計算モデルを記述できることになる．さらに，このGQTMを考えることにより，量子計算における計算の複雑さを定義することができ，厳密な計算量を導出することができる．これを用いて，OMV-SATアルゴリズムの計算量が求められており，量子アルゴリズムと，ある増幅過程を用いれば，NP完全問題が多項式解けるということが示されている[1, 2, 3, 8]．

本講演では，まずGQTMの定義と，計算過程を説明し．言語クラスとその包含関係を説明する．そして，一般的な部分再帰関数を重ね合わせ状態を用いて計算するときの問題を説明し，それを計算するUQTMのコード生成における計算の複雑さを求める．さらに，Looping問題に対するBVの定理をLQTMを用いた場合に拡張し，それを用いて，部分再帰関数の計算を重ね合わせ状態に対して行うLQTMのコード生成における計算の複雑さを求める．

2 一般化量子チューリング機械

GQTM M_{gq} は，次の 4 つ組 $(Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ で与えられる．ここで，Λ_δ は様相（configuration）から様相への量子遷移関数，Q と Σ はそれぞれ標準的な基底 $\{|q\rangle ; q \in Q\}$ と $\{|a\rangle ; a \in \Sigma\}$ によって張られるヒルベルト空間 $\mathcal{H}_Q$ と $\mathcal{H}_\Sigma$ 上の密度作用素の集合である．テープ状態 A は，Σ の要素からなる配列で標準的な基底 $\{|A\rangle ; A \in \Sigma^*\}$ によって張られるヒルベルト空間 $\mathcal{H}_\Sigma$ 上の密度作用素で表される．ここで Σ^* はアルファベット Σ の要素のすべての配列である．テープの位置は標準的な基底 $\{|i\rangle ; i \in \mathbb{Z}\}$ によって張られるヒルベルト空間 $\mathcal{H}_Z$ 上の密度作用素で表される．GQTM M_{gq} の様相 ρ はヒルベルト空間 $\mathcal{H} \equiv \mathcal{H}_Q \otimes \mathcal{H}_\Sigma \otimes \mathcal{H}_Z$ 上の密度作用素で表される．ここで，$\mathfrak{S}(\mathcal{H})$ を $\mathcal{H}$ 上のすべての密度作用素の集合とする．

次の遷移関数 δ_1 を考える．

$$\begin{aligned}\delta_1 : \mathbb{R} \times Q \times \Sigma \times Q \times \Sigma \times Q \times \Sigma \times \{0, \pm 1\} \times Q \times \Sigma \times \{0, \pm 1\} \\ \to \mathbb{C}.\end{aligned}$$

量子遷移関数は次の準線形完全正チャネルで与えられる．

$$\Lambda_\delta : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\mathcal{H}),$$

これは，次の条件を満たす．

定義 1 すべての様相 $\rho = \sum_k \lambda_k |\psi_k\rangle \langle\psi_k|, |\psi_k\rangle = \sum_l \alpha_{k,l} |q_{k,l}, A_{k,l}, i_{k,l}\rangle, \sum_k \lambda_k = 1, \forall \lambda_k \geq 0,$
$\sum_l |\alpha_{k,l}|^2 = 1, \forall \alpha_{k,l} \in \mathbb{C}$ に対して，遷移関数 δ_1 が存在して，Λ_δ が次のように書け，RHS が状態となるとき，Λ_δ は量子遷移関数と呼ばれる．

$$\begin{aligned}\Lambda_\delta(\rho) = \sum_{k,l,m,n,p,b,d,p',b',d'} & \delta_1(\lambda_k, q_{k,l}, A_{k,l}(i_{k,l}), q_{m,n}, \\ & A_{m,n}(i_{m,n}), p, b, d, p', b', d') \\ & \times |p, B, i_{k,l} + d\rangle \langle p', B', i_{m,n} + d'|\end{aligned}$$

$$B(j) = \begin{cases} b & j = i_{k,l} \\ A_{k,l}(j) & otherwise \end{cases}$$

$$B'(j) = \begin{cases} b' & j = i_{m,n} \\ A_{m,n}(j) & otherwise \end{cases}$$

定義 2 すべての様相 ρ_k に対して，遷移関数

$$\begin{aligned}\delta_2 : Q \times \Sigma \times Q \times \Sigma \times Q \times \Sigma \times \{0, \pm 1\} \times Q \times \Sigma \times \{0, \pm 1\} \\ \to \mathbb{C}\end{aligned}$$

が存在して，Λ_δ が次のように書け，

$$\Lambda_\delta(\rho_k) = \sum_{k,l,m,n,p,b,d,p',b',d'} \delta_2(q_{k,l}, A_{k,l}(i_{k,l}), q_{m,n},$$
$$A_{m,n}(i_{m,n}), p, b, d, p', b', d')$$
$$\times |p, B, i_{k,l}+d\rangle\langle p', B', i_{m,n}+d'|$$

RHS が状態であるとき，$M_{gq} = (Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ はＬＱＴＭと呼ばれる．すべての様相 $\sum_k \lambda_k \rho_k$ に対して，Λ_δ は次のアフィン性をもつ;

$$\Lambda_\delta\left(\sum_k \lambda_k \rho_k\right) = \sum_k \lambda_k \Lambda_\delta(\rho_k)$$

定義 3 Λ_δ がユニタリーチャネル：$\Lambda_\delta = Ad_{U_\delta}$ であるとき，$GQTM$ M_{gq} は $UQTM$ と呼ばれる．ここで，$|\psi\rangle = |q, A, i\rangle$ に対して U_δ は次のようになる．

$$U_\delta|\psi\rangle = U_\delta|q, A, i\rangle$$
$$= \sum_{p,b,r} \delta_3(q, A(i), p, b, d)|p, B, i+d\rangle$$

ここで

$$\delta_3 : Q \times \Sigma \times Q \times \Sigma \times \{0,1\} \to \mathbb{C}$$

はすべての $q \in Q, a \in \Sigma$, $q'(\neq q) \in Q, a'(\neq a) \in \Sigma$ に対して次を満たす．

$$\sum_{p,b,d} |\delta_3(q, a, p, b, d)|^2 = 1.$$

$$\sum_{p,b,d,d'} \delta_3(q', a', p, b, d')^* \delta_3(q, a, p, b, d) = 0.$$

[1, 2] において，SAT 問題を多項式時間で解くために用いられるカオス増幅器は，非線形チャネルであり，[7] で GQTM による表現がなされている．

2.1 GQTM の計算過程

$M = (Q, \Sigma, \mathcal{H}, \Lambda_\delta)$，$\rho_0 = |\psi_0\rangle\langle\psi_0|$，$|\psi_0\rangle = |q_0, A, 0\rangle$ とする．A の初期状態を M の入力と呼ぶ．GQTM における計算過程は Λ_δ を初期様相 ρ_0 に及ぼすことにより進行し，プロセッサ状態が終状態の集合 $\{q_F\}$ に入るまで繰り返され，停止する．この過程は，Λ_δ を用いて次のように記述される．

$$\Lambda_\delta \circ \cdots \circ \Lambda_\delta(\rho_0) = \rho_f$$

ρ_f は終状態で，次のように表される．

$$\rho_f = \sum_k \lambda_k \rho_k + \sum_l \mu_l \sigma_l$$

$$\sum_k \lambda_k + \sum_l \mu_l = 1, \quad \forall \lambda_k, \mu_l \geq 0$$

ここで，$\sigma_l \uparrow H_Q \in \{q_F\}$ である．$p = \sum_l \mu_l$ は停止確率とよばれる．

2.2 GQTM における言語クラス

本節では，GQTM を用いて定義される言語クラスを説明する．L をアルファベット列とする．$x \in L$ で停止し，$x \notin L$ で停止しない TM（または GQTM) が存在するとき，L を言語といい，M は L を認識するという．

定義 4 言語 L に対しある *GQTM*（*UQTM*, *LQTM*）M_{gq} が存在し，M_{qg} は L を多項式時間で確率 $p \geq \frac{1}{2}$ で停止するとき，L はクラス *BGQPP*（*BUQPP* = *BPP*, *BLQPP*）に属する．

LQTM は CTM を含むことから，次の包含関係が成り立つ．

$$BPP \subseteq BLQPPL \subseteq BGQPP.$$

さらに，[7] において次が示されている．

定理 5 *NP*⊆*BGQPP*

2.3 Looping 定理の GQTM での拡張

UQTM における Looping 定理は [6] で示されており，そこでは，停止回数 N を入力とし，あるプロセッサ状態 q について，q にちょうど N 回入るような UQTMM_U を構成できることが示されている．

いま，$M_L = (Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ を LQTM，初期様相を ρ_0 とする．ステップ数 N 後に様相が

$$\Lambda_\delta^N(\rho_0) = \sum_k p_k \rho_k$$

$$\sum_k p_k = 1, \forall k, p_k \geq 0$$

であるとする．このとき，次の定理が成り立つ [10].

定理 6 (Looping Theorem) 任意のステップ数 N と ρ_k に対して，N ステップの間，ρ_k を保持し，その他の $\rho_l, (l \neq k)$ に対して，M_L が動作を続けるような *LQTM*M'_L が存在する．

3 部分再帰関数に対するGQTM

この節では，部分再帰関数を計算するUQTMが重ね合わせ状態を入力としたときに生じる問題と，その問題を回避するようなUQTMのコードを生成するCTMの計算時間について議論する[10].

まず，$g:\Sigma\to\Sigma$ と $h:\Sigma\to\{0,1\}$ を計算可能な関数，$f:\Sigma\to\Sigma$ を計算可能な部分再帰関数として，次のように定義する.

$$f(x)=\begin{cases} f(g(x)) & h(x)=1 \\ x & h(x)=0 \end{cases}$$

入力を x として，$f(x)$ を計算するCTMM を次のように書く.

$$M(x)=f(x).$$

いま，$M(x)$ の計算時間は，予め判らないものとする．一般的に，部分再帰関数の計算時間 N はいつ $h(x)=0$ となるか計算が実行されるまで決定されず，関数内でのループの回数に依存している.

ここで，入力 x に対して $f(x)$ を計算するUQTM M_U とLQTM M_L を考える．$f(x)$ は計算可能であるから，全ての入力 x に対してこれを計算するCTMが存在し，Deutchの定理より，同様の動作をする M_U と M_L も存在する．そして，これは，M_U と M_L のコードを生成するCTMM' が存在することと同義である．いま M_U と M_L のコードをそれぞれ $<M_U>,<M_L>$ と書く．また，入力 x に対するTMM の計算時間 $T(M(x))$ を N_x と書く．一般的に，x と異なる入力 y について，$N_y\neq N_x$ である.

U_δ を，M_U での計算に用いられるユニタリー作用素とする．入力 x に対して,N_x ステップ後の様相は,

$$\begin{aligned} M_U(x) &= (U_\delta)^{N_x}|q_0,x,0\rangle\langle q_0,x,0|(U_\delta^*)^{N_x} \\ &= |q_f,f(x),0\rangle\langle q_f,f(x),0| \end{aligned}$$

となる．一方，入力 y について,N_y ステップ後の様相は

$$\begin{aligned} M_U(y) &= (U_\delta)^{N_y}|q_0,y,0\rangle\langle q_0,y,0|(U_\delta^*)^{N_y} \\ &= |q_f,f(y),0\rangle\langle q_f,f(y),0| \end{aligned}$$

となる，ここで，次のような入力状態を考える.

$$\rho_0=|\psi\rangle\langle\psi|$$

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|q_0,x,0\rangle+|q_0,y,0\rangle).$$

N_x ステップ後の M_U の様相は,

$$(U_\delta)^{N_x}\rho_0(U_\delta^*)^{N_x}=|\psi'\rangle\langle\psi'|$$

$$|\psi'\rangle = \frac{1}{\sqrt{2}}\left(|q_f, f(x), 0\rangle + (U_\delta)^{N_x}|q_0, y, 0\rangle\right)$$

となる，ここで，状態ベクトル $(U_\delta)^{N_x}|q_0, y, 0\rangle$ は不明な状態ベクトルである．また，同じ入力 ρ_0 に対して，N_y ステップ後の様相は，

$$(U_\delta)^{N_y}\rho_0(U_\delta^*)^{N_y} = |\psi''\rangle\langle\psi''|$$

$$|\psi''\rangle = \frac{1}{\sqrt{2}}\left((U_\delta)^{N_y}|q_0, x, 0\rangle + |q_f, f(y), 0\rangle\right)$$

となり，ここで，$(U_\delta)^{N_y}|q_0, x, 0\rangle$ は不明な状態ベクトルである，$|q_f, f(x), 0\rangle$．

次の一般的な入力状態

$$\rho = |\phi\rangle\langle\phi|$$

を考える．ここで，$|\phi\rangle = \sum_i^n \alpha_i |q_0, x_i, 0\rangle$，$\sum_i^n |\alpha_i|^2 = 1$，$\forall\alpha_i \in \mathbb{C}$，$n \in \mathbb{N}$，$n < +\infty$ である．これは，純粋状態で，重ねあわせ状態である．$i = 1, \cdots, n$ に対して，$N_{x_i} = T(M(x_i))$ とし，F_N を次を満たす $\{1, \cdots, n\}$ の部分集合とする．

$$F_N = \left\{i \middle| (U_\delta)^N |q_0, f(x_i), 0\rangle = |q_f, f(x_i), 0\rangle\right\}.$$

N_{x_j} ステップ後の様相は，

$$(U_\delta)^{N_{x_j}}\rho(U_\delta^*)^{N_{x_j}} = |\phi_j'\rangle\langle\phi_j'|$$

となり，ここで

$$|\phi_j'\rangle = \sum_{k\in F_{N_{x_j}}} \alpha_k |q_f, f(x_k), 0\rangle + \sum_{l\notin F_{N_{x_j}}} \alpha_l (U_\delta)^{N_{x_j}} |q_0, x_l, 0\rangle$$

である．

重ね合わせ状態の入力に対し，それぞれの入力 x_i の計算時間のずれから，M_U はそれぞれの x_i に対し，ちょうど N_{x_i} ステップ後に $f(x_i)$ の計算結果を保持している．いま，あるステップ数 N 時間後に全ての重ね合わせ状態に対して，同時に計算が終了するような UQTM を考える．

M_{US} を任意の重ねあわせ状態 $\rho = |\phi\rangle\langle\phi|$ の入力に対し，ステップ数 N が存在し，

$$(U_\delta)^N \rho (U_\delta^*)^N = |\phi'\rangle\langle\phi'|$$

$$|\phi'\rangle = \sum_i^n \alpha_i |q_f, f(x_i), 0\rangle$$

となる UQTM とする．次の定理が示されている [10].

定理 7 入力として $< M(f(x)) >, N$ を受け取り，$< M_{US} >$ を出力する TMM' ($\langle M \rangle$) が存在し，その計算時間は

$$T(M') \approx \sum_{i}^{n} T(M(x_i))$$

となる．ここで，$T(M(x_i))$ は，入力 x_i に対する M の計算時間で，$\approx$ は，オーダーの意味で等しいことを表す．

$N_{\max}$ を全ての入力に対する M の計算時間のうち，最大のものとする．同時に計算を終了させるためには，各重ね合わせ状態が，その計算過程において干渉を起こすことなく，かつ，終状態に入ったとき $N_{\max} - N_x$ 回のループを行い，その状態ベクトルを保持し続けなければいけない．このことから，コードを生成する CTM の計算時間は，すべての入力に対し，一旦計算時間を求め，それからループ回数をおのおの求め，計算過程にループを挿入するという工程のため，以上のようになる．

LQTM のコードを生成する場合，計算時間の上限さえ求められれば，各入力に対する正確な計算時間は必要ないため，次の定理が示される．

定理 8 M_L のコードを生成する TMM'' が存在し，その計算時間は

$$T(M'') \approx T(M(x))$$

となる．

参考文献

[1] M.Ohya and I.V.Volovich, *Quantum computing and chaotic amplification*, J. opt. B, **5**,No.6 639-642, 2003.

[2] M.Ohya and I.V.Volovich, *New quantum algorithm for studying NP-complete problems*, Rep.Math.Phys., **52**, No.1,25-33 2003.

[3] M.Ohya and I.V.Volovich, *Quantum information, computation, cryptography and teleportation*, Springer, to appear.

[4] M.Ohya and N.Masuda, *NP problem in Quantum Algorithm,* Open Systems and Information Dynamics, 7 No.1 33-39, 2000.

[5] L. Accardi and M.Ohya, A Stochastic limit approach to the SAT problem, Open systems and Information Dynamics, 11-3, 219-233, 2004

[6] E.Bernstein and U.Vazirani, *Quantum Complexity Theory*, In Proc. 25th ACM Symp. on Theory of Computation, 11–20, 1993.

[7] S.Iriyama, M.Ohya and I.V.Volovich (2006) Generalized Quantum Turing Machine and its Application to the SAT Chaos Algorithm, QP-PQ:Quantum Prob.. White Noise Anal., Quantum Information and Computing, 19, World Sci. Publishing, 204-225

[8] S.Iriyama and M.Ohya, Rigorous Estimate for OMV SAT Algorithm, to appear in OSID, 2008.

[9] S.Iriyama and M.Ohya, Language Classes Defined by Generalised Quantum Turing Machine, TUS preprint, 2008.

[10] S.Iriyama and M.Ohya, The problem to construct Unitary Quantum Turing Machine for compute partial recursive function, TUS preprint, 2008.